Notice of Allowability	Application No. 09/931,558	Applicant(s) POLETTO ET AL.	
	Examiner Minh Dinh	Art Unit 2132	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address--

All claims being allowable, PROSECUTION ON THE MERITS IS (OR REMAINS) CLOSED in this application. If not included herewith (or previously mailed), a Notice of Allowance (PTOL-85) or other appropriate communication will be mailed in due course. **THIS NOTICE OF ALLOWABILITY IS NOT A GRANT OF PATENT RIGHTS.** This application is subject to withdrawal from issue at the initiative of the Office or upon petition by the applicant. See 37 CFR 1.313 and MPEP 1308.

1. ☒ This communication is responsive to *Examiner's amendment authorized on 4/18/06*.

2. ☒ The allowed claim(s) is/are *1-8 and 10-23*.

3. ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
   a) ☐ All b) ☐ Some* c) ☐ None of the:
      1. ☐ Certified copies of the priority documents have been received.
      2. ☐ Certified copies of the priority documents have been received in Application No. _____ .
      3. ☐ Copies of the certified copies of the priority documents have been received in this national stage application from the International Bureau (PCT Rule 17.2(a)).

   * Certified copies not received: _____.

Applicant has THREE MONTHS FROM THE "MAILING DATE" of this communication to file a reply complying with the requirements noted below. Failure to timely comply will result in ABANDONMENT of this application.
THIS THREE-MONTH PERIOD IS NOT EXTENDABLE.

4. ☐ A SUBSTITUTE OATH OR DECLARATION must be submitted. Note the attached EXAMINER'S AMENDMENT or NOTICE OF INFORMAL PATENT APPLICATION (PTO-152) which gives reason(s) why the oath or declaration is deficient.

5. ☐ CORRECTED DRAWINGS (as "replacement sheets") must be submitted.
   (a) ☐ including changes required by the Notice of Draftsperson's Patent Drawing Review (PTO-948) attached
      1) ☐ hereto or 2) ☐ to Paper No./Mail Date _____.
   (b) ☐ including changes required by the attached Examiner's Amendment / Comment or in the Office action of Paper No./Mail Date _____.

Identifying indicia such as the application number (see 37 CFR 1.84(c)) should be written on the drawings in the front (not the back) of each sheet. Replacement sheet(s) should be labeled as such in the header according to 37 CFR 1.121(d).

6. ☐ DEPOSIT OF and/or INFORMATION about the deposit of BIOLOGICAL MATERIAL must be submitted. Note the attached Examiner's comment regarding REQUIREMENT FOR THE DEPOSIT OF BIOLOGICAL MATERIAL.

Attachment(s)

1. ☒ Notice of References Cited (PTO-892)
2. ☐ Notice of Draftperson's Patent Drawing Review (PTO-948)
3. ☐ Information Disclosure Statements (PTO-1449 or PTO/SB/08), Paper No./Mail Date _____
4. ☐ Examiner's Comment Regarding Requirement for Deposit of Biological Material
5. ☐ Notice of Informal Patent Application (PTO-152)
6. ☐ Interview Summary (PTO-413), Paper No./Mail Date _____ .
7. ☒ Examiner's Amendment/Comment
8. ☒ Examiner's Statement of Reasons for Allowance
9. ☐ Other _____.

KAMBIZ ZAND
PRIMARY EXAMINER

EXAMINER'S AMENDMENT

1. An examiner's amendment to the record appears below. Should the changes and/or additions be unacceptable to applicant, an amendment may be filed as provided by 37 CFR 1.312. To ensure consideration of such an amendment, it MUST be submitted no later than the payment of the issue fee.

Authorization for this examiner's amendment was given in a telephone interview with Denis Maloney on 04/14/06.

The application has been amended as follows:

1. (Currently Amended) The data collector of claim 2 wherein the redundant network is a leased line. ~~A data collector comprises:~~

~~a computing device that samples packet traffic over a network, and which accumulates and collects statistical information about the packet traffic on the network; and~~

~~a port to link the data collector over a redundant network that does not carry the packet traffic to deliver the accumulated and collected statistical information about the network packet traffic to a central control center.~~

2. (Currently Amended) A data collector to sample packet traffic, accumulate, and collect statistical information about network flows comprises:

a computing device that executes a computer program product stored on a computer readable medium comprising instructions to cause the computing device to:

collect statistical information pertaining to network packets received by the data collector;

monitor a parameter of traffic flow at multiple levels of granularity to trace the source of an attack, with instructions to monitor further comprising instructions to:

divide the traffic flow into buckets that track counts of how many packets the data collector examines for a given parameter; and

adjust the number of buckets as the number of buckets approaches a bucket threshold, by combining several buckets into fewer buckets or dividing a bucket into more buckets;

maintain the statistical information in a log; and wherein the data collector further comprises:

a port to link the data collector over a redundant network that does not carry the packet traffic to deliver collected statistical information ~~data~~ about the network packets to a central control center upon demand by the central control center.

4. (Currently Amended) The data collector of claim 2 wherein the redundant network is a telephone network ~~or dedicated leased telephone line~~.

7. (Currently Amended) The data collector of claim 2 wherein the computer program product in the data collector executes rules to analyze the collected statistical information ~~statistics~~ and produces a message that raises an alarm to the control center.

11. (Currently Amended) A method of collecting data from sampled network traffic, pertaining to network traffic flows comprises:

sampling the network traffic and generating statistical information pertaining to the sampled network packets; ~~and~~

monitoring a parameter of traffic flow at multiple levels of granularity to trace the source of an attack, with monitoring further comprising:

dividing the traffic flow into buckets that track counts of how many packets a data collector or gateway examines for a given parameter; and

adjusting the number of buckets as the number of buckets approaches a bucket threshold, by combining several buckets into fewer buckets or dividing a bucket into more buckets;

communicating ~~the generated data~~ the generated statistical information over a redundant network that does not carry the packet traffic to deliver the generated statistical information ~~data~~ pertaining to the network packets to a central control center in response to a query for the generated statistical information from the central controller.

12. (Currently Amended) The computer program product of claim 23 wherein layer 3-7 analysis further comprises instructions to:

monitor network traffic for unusual levels of IP fragmentation, or fragmented IP packets with bad or overlapping fragment offsets. ~~The method of claim 11 wherein generating further comprises:~~

~~monitoring a parameter of traffic flow at multiple levels of granularity.~~

13. (Currently Amended) The computer program product of claim 23 wherein layer 3-7 analysis further comprises instructions to:

monitor network traffic for IP packets with bad source addresses or ICMP packets with broadcast destination addresses. ~~The method of claim 12 wherein monitoring the parameter at multiple levels of granularity is used to trace the source of an attack.~~

14. (Currently Amended) The computer program product of claim 23 wherein layer 3-7 analysis further comprises instructions to:

monitor network traffic for transport control protocol (TCP) or user datagram protocol (UDP) packets addressed to unused ports. ~~The method of claim 13 wherein monitoring further comprises:~~

~~dividing the traffic flow into buckets that track counts of how many packets a data collector or gateway examines for a given parameter; and~~

~~adjusting the number of buckets as the number of buckets approaches a bucket threshold, by combining several buckets into fewer buckets or dividing a bucket into more buckets.~~

21. (Currently Amended) A computer program product residing on a computer readable medium for sampling network packet traffic to accumulate, and collect statistical information about network flows, comprises instructions for causing ~~the~~ a device to:

collect network packets and produce statistical information pertaining to collected network packets;

monitor a parameter of traffic flow at multiple levels of granularity to trace the source of an attack, with instructions to monitor further comprising instructions to:

divide the traffic flow into buckets that track counts of how many packets a data collector or gateway examines for a given parameter;

adjust the number of buckets as the number of buckets approaches a bucket threshold, by combining several buckets into fewer buckets or dividing a bucket into more buckets;

parse information in the collected packets and maintain the information in a log; and

send the ~~statistics~~ statistical information to a central control center over a redundant network that does not carry the packet traffic in response to a query from the central controller.

22. (Currently Amended) The computer program product of claim 9 wherein layer 3-7 analysis further comprises instructions to:

monitor network traffic for transmission control protocol (TCP) packets with unusually small window sizes, which indicate server loading due to an attack, or transmission control protocol (TCP) ACK packets that do not belong to a known connection. ~~The computer program product of claim 21 further comprising instructions to:~~

~~monitor a parameter of traffic flow at multiple levels of granularity to trace the source of an attack, with instructions to monitor further comprising instructions to:~~

~~divide the traffic flow into buckets that track counts of how many packets a data collector or gateway examines for a given parameter; and~~

~~adjust the number of buckets as the number of buckets approaches a bucket threshold, by combining several buckets into fewer buckets or dividing a bucket into more buckets.~~

23. (New) The computer program product of claim 21 further comprising instructions to: apply multi-level analysis to monitor TCP packet ratios, repressor traffic and statistical information based on Layer 3-7 analysis.

2. The following is an examiner's statement of reasons for allowance. The present invention is directed to a method and device for collecting network information in order to detect denial of service (DOS) attacks. More specifically, independent claims 2, 11 and 21 identify the uniquely distinct features: monitoring a parameter of traffic flow at multiple levels of granularity to trace the source of an attack, with monitoring further comprising: dividing the traffic flow into buckets that track counts of how many packets a data collector or gateway examines for a given parameter; and adjusting the number of buckets as the number of buckets approaches a bucket threshold, by combining several buckets into fewer buckets or dividing a bucket into more buckets. The closest prior art, Mansfield et al. ("Towards Trapping Wily Intruders in the Large"), also disclose a method for monitoring network traffic and detecting a DOS attack when the count of a certain type of packets reaches a threshold. However, Mansfield does not teach dividing the traffic flow into buckets that track counts of how many packets a data collector examines for a given parameter and adjusting the number of buckets as the number of buckets approaches a bucket threshold, by combining several buckets into fewer buckets or dividing a bucket into

more buckets. The prior art, taken either singly or in combination, fails to anticipate or fairly suggest the limitations of applicant's independent claim, in such a manner that a rejection under 35 U.S.C 102 or 103 would be proper. The claimed invention is therefore considered to be in condition for allowance as being novel and nonobvious over prior art.

Any comments considered necessary by applicant must be submitted no later than the payment of the issue fee and, to avoid processing delays, should preferably accompany the issue fee. Such submissions should be clearly labeled "Comments on Statement of Reasons for Allowance."

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Minh Dinh whose telephone number is 571-272-3802. The examiner can normally be reached on Mon-Fri: 10:00am-6:30pm.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Gilberto Barron can be reached on 571-272-3799. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

MD

Minh Dinh
Examiner
Art Unit 2132

KAMBIZ ZAND
PRIMARY EXAMINER

MD
4/18/06